IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

| | |
|---|---|
| In re: Clearview AI, Inc. Consumer Privacy Litigation | Civil Action File No.: 1:21-cv-00135<br>Judge Sharon Johnson Coleman<br>Magistrate Judge Maria Valdez |

**PLAINTIFFS' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION**

## INTRODUCTION

Without providing notice or receiving consent, Defendants Clearview AI, Inc. ("Clearview"); Hoan Ton-That; and Richard Schwartz (collectively, "Defendants"): (a) scraped billions of photos of people's faces from the internet; (b) harvested the subjects' biometric identifiers and information (collectively, "Biometric Data"); and (c) created a searchable database of that data (the "Biometric Database") which they made available to private entities, friends and law enforcement in order to earn profits. Defendants' conduct violated, and continues to violate, Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, and tramples on Illinois residents' privacy rights. Unchecked, Defendants' conduct will cause Plaintiffs David Mutnick, Mario Calderon, Jennifer Rocio, Anthony Hall and Isela Carmean and Illinois class members to suffer irreparable harm for which there is no adequate remedy at law.

Defendants have tacitly conceded the need for injunctive relief. In response to Plaintiff Mutnick's preliminary injunction motion in his underlying action, Defendants desperately sought to avoid judicial oversight by claiming to have self-reformed. But Defendants have demonstrated that they cannot be trusted. While Defendants have represented that they were cancelling all non-law enforcement customer accounts, a recent patent application reveals Defendants' commercial aspirations. Further, while Defendants contend that Illinois residents can opt out of the Biometric Database, the opt-out process is a ruse that actually forces Illinois residents to consent to Defendants' collection of their Biometric Data. Illinois residents' should not be forced to provide Defendants with the very information Defendants stole in the first instance in order to get out of a database they never consented to being a part of.

Based on Defendants' above-described conduct and a history of lax security practices, Plaintiffs seek to enjoin Defendants from:

(a) Continuing to possess, use and store the unlawfully collected biometric identifiers and biometric information (collectively, "Biometric Data") of Illinois residents;

(b) Collecting, capturing or obtaining Illinois residents' Biometric Data without first providing the notice and obtaining the releases required by Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*;

(c) Selling, trading leasing or otherwise profiting from Illinois residents' Biometric Data; and

(d) Distributing, redistributing or disseminating Illinois residents' Biometric Data without obtaining the consent required by BIPA.

Any preliminary injunctive relief should also require Defendants to:

(a) Store, transmit and protect from disclosure all Biometric Data of Illinois residents: (i) using the reasonable standard of care within Defendant Clearview's industry; and (ii) in a manner that is the same as or more protective than the manner in which the Clearview Defendants store, transmit and protect other confidential and sensitive information; and

(b) Develop and publish on Defendant Clearview's website a written policy, made available to the public, that establishes a retention schedule and guidelines for permanently destroying Illinois residents' Biometric Data when the initial purpose for collecting or obtaining such Biometrics has been satisfied or within three years of the Illinois resident's last interaction with the private entity, whichever occurs first.

The collective relief requested in this paragraph is hereinafter referred to as the "Injunctive Relief." Plaintiffs further request the appointment of a Special Master to assist with the implementation of any Injunctive Relief and to verify Defendants' compliance with any injunction order.

## BACKGROUND FACTS

### *The Parties*

Plaintiffs are Illinois residents whose faces have appeared on various websites on the internet. *See* Dkt. 29 ¶¶ 43-47. Clearview is a Delaware corporation founded by Ton-That and

Schwartz. *Id.*, ¶¶ 13-15. Defendants have provided the Biometric Database – consisting of over three billion biometrically-scanned and searchable images – to public and private entities.[1]

***BIPA***

BIPA strictly regulates an individual's biometric identifiers and information. *See* 740 ILCS 14/1, *et seq.* Under BIPA, biometric identifiers include a "scan of . . . face geometry," and biometric information is "any information . . . based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

In enacting BIPA, the Illinois General Assembly recognized that Biometric Data is sensitive and unique because it cannot be changed if compromised:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information . . . . Biometrics . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

740 ILCS § 14/5(c).

***Defendants' Biometric Database***

Defendants have scraped over three billion facial images from the internet and scanned the facial geometry – *i.e.*, the Biometric Data – of each individual.[2] Defendants also built a searchable database of the scanned images – the Biometric Database – thereby enabling database users to

[1] Luke O'Brien, *The Far-Right Helped Create the World's Most Powerful Facial Recognition Technology*, HuffPost (Apr. 7, 2020) ("*The Far-Right Helped Create Clearview*"), https://www.huffpost.com/entry/clearview-ai-facial-recognition-alt-right_n_5e7d028bc5b6cb08a92a5c48 (last accessed on Apr. 9, 2021); Ryan Mac, *et al.*, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's Walmart, and the NBA*, Buzzfeed News (Feb. 27, 2020) ("*Clearview's Facial Recognition App Use"*), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement (last accessed on Apr. 9, 2021).

[2] *The Far-Right Helped Create Clearview, supra.*

instantly identify unknown individuals using nothing more than a photo.[3] Clearview has boasted that it adds 40 to 50 million new images to the Biometric Database each day. Exhibit 1 (10/8/2019 Clearview email).

Ton-That has described the Biometric Database as "a search engine for faces."[4] According to Ton-That, a person with access to the database can upload thereto a face image of an unknown person, and the database will then: (a) match that face with images in the database; and (b) provide the user with information Defendants have amassed about the person.[5] Over 500,000 face searches have been performed by public and private individuals and entities, including: (a) 8,900 by the Illinois Secretary of State; (b) 7,500 by U.S. Customs and Border Patrol; and (c) more than 8,000 by Immigration and Customs Enforcement.[6]

Defendants do not notify individuals that their Biometric Data is contained in the Biometric Database. Dkt. 29 ¶¶ 1, 60. Defendants do not seek Illinois residents' consent to perform biometric scans on their images, *see id.*, other than in connection with forcing a resident to consent in order to nominally "opt out" of the database, as described above and further discussed below.

***The Dangers of the Biometric Database***

United States Senator Edward J. Markey has highlighted the grave dangers the Biometric Database poses to the public's civil liberties and privacy: "Clearview's product appears to pose particularly chilling privacy risks" and could be "capable of fundamentally dismantling

---

[3] Donie O'Sullivan, *Clearview AI's Founder Hoan Ton-That Speaks Out [Extended Interview]*, CNN Business (Mar. 6, 2020) ("*Clearview's Founder Speaks Out*"), https://www.youtube.com/watch?v=q-1bR3P9RAw (last accessed on Apr. 9, 2021).
[4] Neil Cavuto, *New Facial Recognition Tech 'Loved' by Law Enforcement: Clearview AI CEO*, Fox Business (Feb. 19, 2020) (*"New Facial Recognition Tech"*), https://video.foxbusiness.com/v/6133890195001/#sp=show-clips (last accessed on Apr. 9, 2021).
[5] *Id.*
[6] *Clearview's Facial Recognition App Use, supra*; *see also* Ryan Mac, *et al.*, *Surveillance Nation*, Buzzfeed News (Apr. 6, 2021), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition (last accessed on Apr. 9, 2021).

Americans' expectation that they can move, assemble, or simply appear in public without being identified."[7] Moreover, according to Senator Markey, a criminal could use the technology to find out where "someone walking down the street lives or works" or a foreign adversary could "gather information about targeted individuals for blackmail purposes."[8] Relatedly, Joy Buolomwini, the author of a seminal study on racial and gender bias in facial recognition technology,[9] has recently highlighted the disproportional harm mass surveillance via facial recognition can have on certain populations: "When these [algorithmic] systems are used as tools of mass surveillance, the excoded, those who are harmed by algorithmic systems, suffer the brunt of overpolicing, undue scrutiny, and false arrests."[10]

Defendants have allowed hundreds of for-profit businesses and non-law enforcement entities to access the Biometric Database, including Macy's Best Buy, Walmart, Bank of America, the NBA and a sovereign wealth fund owned by the government of Abu Dhabi[11] and have taken steps to make their technology commercially available.[12] Macy's employees, alone, conducted

---

[7] Hon. Edward J. Markey letter to Hoan Ton-That (Jan. 23, 2020) (the "Jan. 23, 2020 Sen. Markey Letter"), https://www.markey.senate.gov/imo/media/doc/Clearview%20letter%202020.pdf (last accessed on Apr. 9, 2021); *see also* Hon. Edward J. Markey letter to Hoan Ton-That (Mar. 3, 2020) (the "Mar. 3, 2020 Sen. Markey Letter), https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20Clearview%20II%203.3.20.pdf (last accessed on Apr. 9, 2021).

[8] *Id.*

[9] Joy Buolamwini, *et al.*, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1–15, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (last accessed on Apr. 7, 2021).

[10] *Surveillance Nation*, *supra.*

[11] *Clearview's Facial Recognition App Use*, *supra.*; Ryan Mac, *et al.*, *Secret Users of Clearview AI's Facial Recognition Dragnet Included a Former Trump Staffer, a Troll, and Conservative Think Tanks*, Buzzfeed News (Mar. 25, 2020) ("*Secret Users of Clearview"*), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-trump-investors-friend-facial-recognition (last accessed on Apr. 9, 2021).

[12] Caroline Haskins*, et al.*, *The Facial Recognition Company that Scraped Facebook and Instagram Photos Is Developing Surveillance Cameras*, Buzzfeed News (Mar. 2, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/clearview-facial-recognition-insight-camera-glasses (last accessed on Apr. 9, 2021).

over 6,000 face searches.[13] Further, hundreds of individuals to whom Defendants granted access to the Biometric Database have collectively conducted over 30,000 face searches.[14] Included among those individuals was an alt-right extremist and purported Holocaust denier who has been accused of using the Biometric Database to identify a person sitting next to him on an airplane.[15] Clearview has also granted database access to a number of right-wing activists, Republican members of Congress, Republican party power brokers and conservative organizations.[16] That access could allow political organizations to conduct opposition research at an unprecedented level – namely, it provides the ability to identify who attends an opponent's rallies, as well as the attendees' friends, families, addresses and other personal information. It has been reported that Defendants Clearview and Ton-That have "deep, longstanding ties to far-right extremists."[17]

Regarding law enforcement, Defendants have encouraged law enforcement officers to "run wild" with their use of the Biometric Database and have frequently granted access to the database for free.[18] Even after various police departments banned or explicitly declined to use the Biometric Database, individual officers in those departments continued to conduct thousands of searches using Defendants' software application.[19] That was no accident; Defendants allowed individual officers to continue accessing the Biometric Database even after their superiors had decided not to

---

[13] *Clearview's Facial Recognition App Use, supra.*
[14] *Secret Users of Clearview, supra*.
[15] *Secret Users of Clearview, supra.*
[16] *Secret Users of Clearview, supra.*
[17] *The Far-Right Helped Create Clearview, supra.*
[18] Ryan Mac, *et al.*, *Clearview AI Once Told Cops to "Run Wild" With Its Facial Recognition Tool. It's Now Facing Legal Challenges*, Buzzfeed News (Jan. 28, 2020) ("*Cops Run Wild*"), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-cops-run-wild-facial-recognition-lawsuits (last accessed on Apr. 2, 2020); *see also Surveillance Nation*.
[19] Craig McCarthy, *Rogue NYPD Cops Are Using Facial Recognition App Clearview*, New York Post (Jan. 23, 2020) ("*NYPD Cops Use Clearview*"), https://nypost.com/2020/01/23/rogue-nypd-cops-are-using-sketchy-facial-recognition-app-clearview/ (last accessed on Apr. 2, 2020); *Secret Users of Clearview, supra.*

use the technology.[20] Indeed, on April 6, 2021, it was reported that often there is no official oversight of individual officers' use of the database.[21] As such, there is no way for the public know if the database truly is being used for a governmental purpose or even by a government official.

Based on the above, Clearview's contention that it limits use of the Biometric Database to law enforcement,[22] is illusory – the claim cannot be verified. Moreover, law enforcement's use of the database raises serious concerns. It recently was reported that Clearview's technology fails to accurately identify subjects and even identified two computer-generated images of females of color as actual persons.[23] Further, law enforcement use of the database requires an officer to provide Defendants with real-time information about an investigation, giving rise to the fear that Defendants will misuse the information or share it with others, such as potential employers.

***Defendants' Lax Security Practices***

Defendants have a history of lax security practices which has caused Senator Markey to question whether Defendants can keep the Biometric Database secure.[24] In response to a data breach that exposed Clearview's customer list, Clearview merely stated, "Unfortunately, data breaches are part of life in the 21st century."[25] The response was not surprising, as Defendant Ton-That is a hacker, himself.[26]

Worse, after a third-party discovered that Defendants had a severe data security defect that "exposed [Clearview's ] internal files, apps and source code" and allowed anyone on the internet

---

[20] *See Cops Run Wild, supra; NYPD Cops Use Clearview, supra.*
[21] *Surveillance Nation, supra.*
[22] *New Facial Recognition Tech, supra.*
[23] *See Surveillance Nation, supra*.
[24] Mar. 3, 2020 Sen. Markey Letter, *supra.*; *see also* Mar. 3. 2020 Congressional Letter, *supra.*
[25] Betsy Swan, *Facial-Recognition Company that Works with Law Enforcement Says Entire Client List Was Stolen*, The Daily Beast (Feb. 26, 2020) ("*Clearview Client List Stolen*"), https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen (last accessed on Apr. 9, 2021).
[26] *The Far-Right Helped Create Clearview, supra.*

to access the Biometric Data in the Biometric Database, Defendants tried to cover-up the problem.[27] Specifically, Defendants attempted to pay off the person who discovered the defect in return for his silence.[28] When confronted about the security defect and its discovery, Ton-That conceded that Clearview "'experienced a constant stream of cyber intrusion attempts . . . .'"[29]

***Defendants' Failed Attempts to Self-Correct***

Conceding the need for injunctive relief, after Plaintiff Mutnick filed his preliminary injunction motion, Clearview claimed to have "voluntarily changed its business practices to avoid including data from Illinois residents and to avoid transacting with non-governmental customers anywhere." *Mutnick* Dkt. 56 at 4.[30] In summary, Defendants' stated that they would: (a) try to avoid obtaining photographs and Biometric Data of Illinois residents; (b) implement "an opt-out mechanism to exclude photos from Clearview's database"; and (c) cancel the accounts of non-law enforcement/government entities. *See id.* Defendants submitted the declaration of Clearview's General Counsel in support of their purported changes. *See id.* Notably, Defendants did not agree to: (a) stop scraping photos from the internet; (b) comply with BIPA's notice and consent provisions; or (c) delete all photos and Biometric Data of Illinois residents. *See id.*

While Defendants represented that they would only work with governmental agencies, shortly after making that representation, Defendants filed a patent application that describes a much broader use of their technology.[31] According to the application, "[i]n many instances it may be desirable for an individual to know more about a person that they meet, such as through

---

[27] Zack Whittaker, *Security Lapse Exposed Clearview AI Source Code*, Tech Crunch (Apr. 16. 2020), https://techcrunch.com/2020/04/16/clearview-source-code-lapse (last accessed on Apr. 9, 2021).
[28] *Id.*
[29] *Id.*
[30] Citations to docketed entries are to the CM/ECF-stamped page numbers.
[31] *See* Clearview AI, Inc. Patent Application dated Aug. 7, 2020, http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&f=G&l=50&p=1&r=1&s1=20210042527.PGNR.&u=%2Fnetahtml%2FPTO%2Fsrchnum.html (last accessed on Apr. 7, 2021), attached hereto as Exhibit 2.

business, dating, or other relationship" and, in some instances, "the individual needs to know the information about a newly met person right away to determine whether the person is being honest or has the background as asserted."[32] The application further provides that, the Biometric Database "presents a method for providing information about a person (*e.g.*, an unknown person, a newly met person, a person with deficient memory)."[33]

Moreover, while Defendants represented that they would implement an "opt-out mechanism," they omitted that the mechanism forces an Illinois resident seeking to "opt out" to: (a) provide Clearview with a photograph from which Clearview will "generate facial vectors"; and (b) consent to the collection of their Biometric Data:

> To fulfill your request, you will have to provide a picture of yourself. Clearview will generate facial vectors from this picture . . . .
>
> * * *
>
> By clicking "I accept", you consent to the collection, use and storage of your biometric data for the purpose of blocking any images of me [sic] that may appear in Clearview search results.[34]

Exhibit 2, hereto, consists of screenshots of the "opt-out" process. It is exactly backwards that a person who never wanted to interact with Defendants is required to provide Clearview with personal information and consent to the harvesting of his/her Biometric Data in order to "opt out."

Finally, as set forth in the briefing on Plaintiff Mutnick's original injunction motion, Clearview's General Counsel cannot be taken at his word. *See Mutnick* Dkt. 64 to 64-9. For instance, it is documented that the General Counsel misrepresented facts to the Illinois Secretary of State in connection with providing that government agency access to the Biometric Database.

---

[32] *Id.*
[33] *Id.*
[34] Clearview's Illinois Opt-Out Request Form, https://clearviewai.typeform.com/to/HDz8tJ (last accessed on Apr. 7, 2021), attached hereto as Exhibit 3.

*See id.* Thus, it is not known what actual steps Defendants have taken to identify Illinois residents in the Biometric Database, to prohibit further collection of Illinois residents' Biometric Data or to ensure that their technology is only used by governmental agencies for governmental work. As evidenced by Exhibit 2 (screenshots of "opt-out" process), Defendants take no precautions to prevent an unauthorized person from uploading a photograph of an Illinois resident and consenting to the collection of that person's Biometric Data as part of Defendant's so-called opt-out process.

## ARGUMENT

### I. Legal Standards

#### A. Preliminary Injunctions

When deciding whether to issue a preliminary injunction, a district court should conduct a two-step analysis. *Turnell v. CentiMark Corp.,* 796 F.3d 656, 661 (7th Cir. 2015). First, the movant "must make a threshold showing that: (1) absent preliminary injunctive relief, he will suffer irreparable harm in the interim prior to a final resolution; (2) there is no adequate remedy at law; and (3) he has a reasonable likelihood of success on the merits." *Id.* at 661-62. If the movant satisfies his burden, the court should then consider: "(4) the irreparable harm the moving party will endure if the preliminary injunction is wrongfully denied versus the irreparable harm to the nonmoving party if it is wrongfully granted; and (5) the effects, if any, that the grant or denial of the preliminary injunction would have on nonparties (the 'public interest')." *Id.* at 662. The court should weigh the "balance of potential harms on a 'sliding scale' against the movant's likelihood of success: the more likely he is to win, the less the balance of harms must weigh in his favor; the less likely he is to win, the more it must weigh in his favor." *Id.* at 662.

To demonstrate a likelihood of irreparable harm, the moving party must show "more than a mere possibility of harm." *Whitaker by Whitaker v. Kenosha Unified Sch. Dist. No. 1 Bd. of*

*Educ.,* 858 F.3d 1034, 1045 (7th Cir. 2017). However, the harm need not occur before injunctive relief is warranted, nor must it be certain to occur. *Id.* Rather, a court may consider harm irreparable where it cannot be fully rectified or prevented by a final judgment. *Id.*

Similarly, a movant need not demonstrate that a remedy at law would be wholly ineffectual. *Id.* He simply must show that any award would be seriously deficient when compared to the harm suffered. *Id.* To demonstrate a likelihood of success, a movant need only show that he has a "better than negligible" chance of succeeding on the merits, an "admittedly low requirement." *Washington v. Indiana High Sch. Athletic Ass'n, Inc.*, 181 F.3d 840, 846 (7th Cir. 1999); *Girl Scouts of Manitou Council, Inc. v. Girl Scouts of the United States of Am.,* 549 F.3d 1079, 1096 (7th Cir. 2008).

**B. BIPA**

BIPA strictly regulates Biometric Data and provides for injunctive relief among other remedies. 740 ILCS 14/1, *et seq.* Pursuant to BIPA, a private entity may not collect, capture or otherwise obtain a person's Biometric Data unless it first: (a) informs the person or his legally authorized representative in writing that the Biometric Data is being collected or stored; (b) informs the person or his legally authorized representative in writing of the specific purpose and length of term for which the Biometric Data is being collected, stored and used; and (c) receives a written release executed by the person or his legally authorized representative. 740 ILCS 14/15(b). Similarly, a private entity may not disclose, redisclose or otherwise disseminate an individual's Biometric Data without first providing written notice and receiving written consent. 740 ILCS 14/15(d). BIPA further prohibits a private entity in possession of Biometric Data from selling, leasing, trading or otherwise profiting from that data. 740 ILCS 14/15(c).

BIPA also requires that a private entity in possession of biometric identifiers or information must "develop a written policy, made available to the public, establishing a retention schedule and

guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a). Finally, BIPA requires an entity that possesses Biometric Data to store, transmit and protect that data from disclosure: (a) using the reasonable standard of care within the entity's industry; and (b) in a manner that is the same as or more protective than the manner which the entity stores, transmits and protects other confidential and sensitive information. 740 ILCS 14/15(e).

## II. The Court Should Grant the Requested Injunctive Relief.

### A. Plaintiffs Have Satisfied Their Threshold Burden.

Plaintiffs have satisfied their threshold burden of showing the need for injunctive relief.

**Irreparable Harm:** Absent preliminary injunctive relief, Plaintiffs and class members will suffer irreparable harm. The Biometric Database poses "particularly chilling privacy risks" and could fundamentally disable "Americans' expectation that they can move, assemble, or simply appear in public without being identified."[35] Further, Defendants continue to store Plaintiffs' and class members' Biometric Data notwithstanding lax security practices that have already resulted in multiple breaches of their electronic systems. As the Federal Trade Commission (the "FTC") declared in connection with a $525-$700 million data breach settlement with Equifax: "The incident at Equifax underscores the evolving security threats confronting both private and government computer systems and actions they must take to shield the personal information of consumers."[36] According to the FTC, protecting consumers' sensitive personal information has

[35] *See* Jan. 23, 2020 Sen. Markey Letter, *supra.*

[36] Federal Trade Commission, *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach* (July 22, 2019) ("*FTC Settlement*"), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related (last

to be a top priority for businesses.[37] Notably, BIPA was enacted out of concern that certain businesses would fail to properly secure biometric identifiers and information.[38]

Contrary to the FTC's directives and BIPA's purpose, Defendants have responded to the two known breaches of their electronic systems with a shrug of the shoulders and by trying to conceal the fact that one of the breaches happened. Plaintiffs and class members should not have to accept Defendants' lax attitude with respect to security, especially given that Defendants had no right to harvest their Biometric Data in the first place. Defendants' history of security lapses and their lax attitude towards security subjects Plaintiffs and class members to the ongoing prospect of injury. *See Whitaker by Whitaker*, 858 F.3d at 1045 (harm need not have yet occurred).

Finally, Defendants' efforts to avoid injunctive relief are largely unverified and unverifiable absent a Court order. Moreover, as discussed, those efforts have actually exacerbated the harm to which Plaintiffs and class members are subjected, essentially tricking Illinois residents into consenting to the harvesting of their Biometric Data. This repugnant conduct demonstrates that Defendants are incapable of correcting their unlawful conduct on their own and will continue to engage in conduct designed to harm Plaintiffs and class members if left unchecked.

**No Adequate Remedy at Law:** Plaintiffs and class members have no adequate remedy at law. Defendants' conduct infringes on Plaintiffs' and class members' civil liberties and privacy; threatens their ability to freely move about society, post photos on the internet or use social media

---

accessed on Apr. 7, 2020); *see also* Federal Trade Commission, *Start With Security: A Guide for Business,* https://www.ftc.gov/system/files/documents/ plain-language/pdf0205-startwithsecurity.pdf (last accessed on Apr. 7, 2020); *Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students*, FBI Alert No. I-091318-PSA (Sept. 13, 2018), https://www.ic3.gov/media/2018/180913.aspx (last accessed on Apr. 7, 2020); *See* Mar. 3, 2020 Sen. Markey Letter.

[37] *See FTC Settlement, supra.*

[38] *See* 740 ILCS § 14/5; Kathleen Foody, *Unique Illinois Privacy Law Leads to $550M Facebook Deal*, Associated Press (Feb. 9, 2020), https://abcnews.go.com/Business/wireStory/unique-illinois-privacy-law-leads-550m-facebook-deal-68861584 (last accessed on Apr. 7, 2020).

with their friends and loved ones without fear of being surveilled; and increases their risk of becoming victims of crimes such as stalking or burglary. As Defendants' patent application makes clear, anyone with access to the Biometric Database can instantly learn personal information about an individual simply by taking a photo. No remedy at law can compensate Plaintiffs and class members for these losses of liberty and privacy or for the fear with which they have to live as long as Defendants continue to violate BIPA with impunity. *See* 740 ILCS 14/20 (providing for injunctive relief).

**Success on the Merits:** Given BIPA's straightforward nature, Plaintiffs and class members have a high likelihood of success on the merits. Defendants cannot dispute that the Biometric Database consists of Plaintiffs' and class members' Biometric Data. Indeed, Defendants' entire business model is premised on collecting, capturing, obtaining, disclosing, disseminating, selling, trading and profiting from the Biometric Data. Further, Defendants cannot dispute that they failed to provide Plaintiffs and class members with the requisite written notices or to obtain the requisite written consents/releases. *See* 740 ILCS 14/15(b), (d). Finally, despite Plaintiff Mutnick having first sought injunctive relief a year ago, Defendants have provided no evidence that they have implemented appropriate and required security practices to protect Plaintiffs' and class members' Biometric Data.

Defendants' efforts to moot the need for injunctive relief fail. Even if the purported actions could be verified and did not further harm Plaintiffs and class members, the "mere cessation of the conduct sought to be enjoined does not moot a suit to enjoin the conduct, lest dismissal of the suit leave the defendant free to resume the conduct the next day." *ADT Sec. Servs. v. Lisle-Woodridge Fire Prot. Dist.*, 724 F.3d 854, 864 (7th Cir. 2013) (internal quotation marks omitted); *see also Friends of the Earth, Inc. v. Laidlaw Envtl. Servs.*, 528 U.S. 167, 189 (2000).

### B. The Secondary Injunction Analysis Favors Plaintiffs and Class Members.

Given the strength of Plaintiffs' and class members' BIPA claims, the harm faced absent injunctive relief need only slightly outweigh any harm to Defendants if an injunction was erroneously entered. *See Turnell*, 796 F.3d at 662. The harms to Plaintiffs and class members described throughout far outweigh any harms to Defendants. By acting now, the Court can ameliorate those harms.

In contrast, Defendants will suffer little to no harm if an injunction is entered in error. An injunction will not impact Defendants' ability to utilize the Biometric Database in 49 other states and around the world. Notably, Defendants have continued to operate after their purported self-imposed "fixes" in response to Plaintiff Mutnick's injunction motion. Further, if Defendants obtain a favorable outcome in this litigation, they easily can add Illinois back to the database.

As for the impact on the public, the analysis is the same as it is for Plaintiffs and class members. Thus, the final factor in the analysis weighs in favor of Plaintiffs and class members.

## III. The Requested Injunctive Relief Is Appropriate.

The requested Injunctive Relief is necessary to ameliorate the irreparable harm created by the Biometric Database. Plaintiffs and class members merely seek compliance with BIPA, which includes proper data security measures, the deletion of improperly obtained Biometric Data and a prohibition on future unlawful collection and use of such data. Given the sensitive nature of the Biometric Data, the requested relief is reasonable.

## CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court enter an order granting Plaintiffs and class members the requested Injunctive Relief.

Dated: April 9, 2021

Respectfully submitted,

By: /s/ Scott R. Drury
SCOTT R. DRURY
*Interim Lead Class Counsel for Plaintiffs*

Mike Kanovitz
Scott R. Drury
**LOEVY & LOEVY**
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900
drury@loevy.com

Scott A. Bursor
Joshua D. Arisohn
**BURSOR & FISHER, P.A.**
888 Seventh Avenue
New York, NY 10019
646.837.7150
scott@bursor.com
jarisohn@bursor.com

Frank S. Hedin (to be admitted *pro hac vice*)
**HEDIN HALL LLP**
Four Embarcadero Center, Suite 1400
San Francisco, California 94104
415.766.3534
fhedin@hedinhall.com

Michael Drew
**NEIGHBORHOOD LEGAL LLC**
20 N. Clark Street #3300
Chicago, Illinois 60602
312.967.7220
mwd@neighborhood-legal.com

Michael Wood
Celetha Chatman
**COMMUNITY LAWYERS LLC**
20 N. Clark Street, Suite 3100
Chicago, Illinois 60602
312.757.1880
mwood@communitylawyersgroup.com
cchatman@communitylawyersgroup.com

Steven T. Webster
Aaron S. Book
**WEBSTER BOOKK LLP**
300 N. Washington, Ste. 404
Alexandria, Virginia 22314
888.987.9991
swebster@websterbook.com

*Other Counsel for Plaintiffs*

**CERTIFICATE OF SERVICE**

I, Scott R. Drury, an attorney, hereby certify that, on April 9, 2021, I filed the foregoing document using the Court's CM/ECF system, which effected service on all counsel of record.

/s/ Scott R. Drury
*Interim Lead Class Counsel for Plaintiffs*